UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

AHMED ABDELLATIF, individually and on behalf of all others similarly situated, Plaintiff, v. AT&T, Inc., Defendant.	Case No. 3:24-cv-00876 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Ahmed Abdellatif ("Plaintiff"), on behalf of himself and all others similarly situated ("Class Members"), files this Class Action Complaint ("Complaint") against Defendant AT&T, Inc. ("AT&T" or "Defendant") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to safeguard and secure the personally identifiable information ("PII") of approximately 73 million customers (7.6 million current customers and 65.4 million former customers),[1] including Plaintiff. The individuals affected are former and current customers of Defendant, whose PII was maintained by Defendant.

2. The data reportedly exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. As a result of

---

[1] *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, THE NEW YORK TIMES (Mar. 30, 2024), https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html.

Defendant's negligence, in approximately 2019 or earlier, cybercriminals were able to gain access to Defendant's data records and access this sensitive and valuable PII (the "Data Breach"). On information and belief, information disclosed in the Data Breach includes but is not limited to names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, and AT&T account numbers and passcodes.[2]

3. AT&T provides its customers with internet, telephone, wireless, and other technology services.[3]

4. According to a media post by Defendant, "AT&T has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance of the data set, which includes personal information such as social security numbers, the source of the data is still being assessed."[4]

5. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes, including opening new financial information in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, and using Class members' PII to target other phishing and hacking intrusions.

---

[2] *See id.*; Bill Toulas, *AT&T faces lawsuits over data breach affecting 73 million customers*, BLEEPING COMPUTER, (Apr. 3, 2024), https://www.bleepingcomputer.com/news/security/atandt-faces-lawsuits-over-data-breach-affecting-73-million-customers/.

[3] *Our Purpose,* AT&T, INC., https://about.att.com/pages/corporate-profile (last visited Apr. 8, 2024).

[4] *AT&T Addresses Recent Data Set Released on the Dark Web*, AT&T, INC. (Mar. 30, 2024), https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html.

6. Defendant owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' PII from unauthorized access and disclosure.

7. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and the harm caused to Plaintiff and Class members as a result. Plaintiff brings this action on behalf of himself and all persons whose PII was exposed as a result of the Data Breach.

8. As a result of the Data Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of financial fraud and identity theft. Plaintiff has been forced to spend uncompensated time and money addressing and attempting to mitigate further harm and injury resulting from the Data Breach. In response to learning his PII was exposed in the Data Breach, Plaintiff spent time and money enrolling in Equifax paid identity theft protection services, which further confirmed that his Social Security information was on the "dark web." Plaintiff has spent substantial time changing all his passwords to other accounts, several of which (such as his personal email account) have been subject to unauthorized, attempted logins from international locations. Plaintiff has also suffered emotionally over the stress resulting from the Data Breach and his substantially increased risk of identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft.

9. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including

improvements to Defendant's data security system, future annual audits, and adequate credit monitoring services funded by Defendant.

10. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

11. Plaintiff Ahmed Abdellatif resides in Jefferson County, Colorado. Plaintiff is a citizen of Colorado. On April 4, 2024, Mr. Abdellatif received an alert from Identity IQ (Exhibit 1) notifying him that his PII was among the information accessed by cybercriminals in the Data Breach.[5]

12. Had Plaintiff known that Defendant would not adequately protect his and Class members' PII, he would not have received services from Defendant or any of its affiliates and would not have provided his PII to Defendant or any of its affiliates.

13. Defendant AT&T, Inc., is a Delaware corporation that maintains its headquarters and principal place of business at 208 S. Akard Street, Dallas, TX 75202. Defendant is a citizen of Texas. The registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) because (a) there are 100 or more Class members, (b) at least one Class member is a

[5] *See* Exhibit 1 - Identity IQ Alert.

citizen of a state that is diverse from Defendant's citizenship, and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

15. This Court has general personal jurisdiction over Defendant because Defendant is a citizen of Texas. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services and accepting and processing payments for those products and services within the State.

16. Venue is proper in the Dallas Division of the Northern District of Texas pursuant to 28 U.S.C. § 1391(b) because Defendant resides in the Dallas Division of the Northern District of Texas, a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendant has its principal place of business in the Dallas Division of the Northern District of Texas.

FACTUAL ALLEGATIONS

Overview of Defendant

17. Defendant is a nationwide cellphone and internet service provider.

18. Plaintiff and Class members are, or were, customers of Defendant.

19. To obtain products and/or services, consumers like Plaintiff and Class members are required to provide Defendant directly with sensitive PII.

20. In the regular course of its business, Defendant collects, stores, and maintains the PII it receives from consumers who utilize Defendant's products and or/services.

21. By creating and maintaining massive repositories of PII, Defendant has provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

The Data Breach and Notice Letter

22. In or about March 2024, the PII of former and current AT&T Customers was stolen.[6]

23. Defendant has not confirmed the name of the cybercriminal group responsible for the Data Breach, but news organizations have reported that in 2021, a cybercriminal group called Shiny Hunters claimed "to have hacked AT&T and attempted to sell the data."[7]

24. Shiny Hunters leaked data samples as proof, but AT&T disputed those allegations, stating that the leaked data did not belong to them.[8]

25. "On March 17, 2024, another threat actor named 'MajorNelson' leaked the entire database on a hacking forum for free, clarifying that it was the same one from Shiny Hunters' attack."[9] Again, AT&T refuted allegations of any data leak and asserted that "there were no signs that its systems had been breached."[10]

26. AT&T finally admitted on March 30, 2024, that the exposed data did, in fact, belong to its customers.[11]

---

[6] *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, *supra* n.1.

[7] Toulas, *supra* n.2.

[8] *Id*.

[9] *Id*.

[10] *Id.*

[11] *Id*.

27. In fact, "this is the first time that AT&T has acknowledged that the leaked data belongs to its customers, some three years after a hacker claimed the theft of 73 million AT&T customer records."[12]

28. The data leaked in the Data Breach includes each affected "person's full name, email address, mailing address, phone number, Social Security number, date of birth, AT&T account number and passcode."[13]

29. While Defendant claims that it "work[s] hard to safeguard your information using technology controls and organizational controls. . . . [,]" that is not so; Defendant failed to secure its systems, which resulted in the aforesaid data breach of 73 million customers.[14]

30. Defendant did not use reasonable security procedures to safeguard the sensitive information of Plaintiff and Class Members.

31. Defendant waited at least three years from the date it learned of the Data Breach to merely conduct an investigation, let alone notify the affected individuals. Defendant has yet to directly notify the affected individuals, including Plaintiff and Class members.

32. To date, Defendant has not disclosed crucial information, including, but not limited to, the identity of the hacking group responsible for the Data Breach; how the cybercriminals were able to exploit vulnerabilities in Defendant's IT security systems; any steps taken by Defendant to

[12] Zack Whittaker, *AT&T resets account passcodes after millions of customer records leak online*, TECHCRUNCH (Mar. 30, 2024), https://techcrunch.com/2024/03/30/att-reset-account-passcodes-customer-data/?guccounter=1.

[13] *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, *supra* n.1.

[14] *AT&T Privacy Notice*, AT&T, INC. (Dec. 11, 2023), https://about.att.com/privacy/privacy-notice.html; *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, *supra* n.1.

safeguard its systems; the identities of the victims of the Data Breach, and any remedial measures Defendant plans to offer to those affected individuals.

33. While Defendant has not disclosed the exact data obtained in the Data Breach, its media post states that the data likely "includes personal information such as social security numbers . . . ."[15]

34. Defendant's systems hacked by cybercriminals contained Plaintiff's and Class members' PII that was accessible, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

35. Plaintiff and Class members provided their PII to Defendant, either directly or indirectly, with the reasonable expectation and mutual understanding that Defendant would comply with its obligation to keep such information confidential and secure from unauthorized access.

36. Defendant also benefited directly from the PII provided by Plaintiff and Class members. As stated in Defendant's publicly available Privacy Policy, Defendant "use[s] the data [it] collect[s] to prevent fraud, and to improve the effectiveness, security, and integrity of the website. [It] also use[s] the data to provide [customers] information about AT&T and its products and services and offers[.]"[16]

37. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

---

[15] *AT&T Addresses Recent Data Set Released on the Dark Web, supra* n.4.
[16] *AT&T Privacy Notice*, *supra* n.14.

Defendant Knew That Criminals Target PII.

38. At all relevant times, Defendant knew or should have known that Plaintiff's and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Defendant should have anticipated and guarded against.

39. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the Data Breach, which has been widely reported in the last few years.

40. Shiny Hunters, the cybercriminal group that is "one of the most recognized threat actors among the hacking community" and infamous for carrying out "sophisticated cyberattacks on over 40 online services across the world," reportedly took responsibility in 2021 for the Data Breach, giving Defendant initial notice of the possibility that its cyber security systems had been breached, or, at the very least, that its systems were a potential target.[17]

41. MajorNelson, another notorious threat actor who leaked the entire database initially stolen by Shiny Hunters onto a hacking forum for free, reportedly took responsibility for the Data Breach on March 17, 2024.[18]

---

[17] Toulas, *supra* n.2.

[18] *Id.*

42. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' PII.[19]

43. As a result of the notoriety of cyberattacks on systems like Defendant's, several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack like the Data Breach.

44. In light of the Shiny Hunters' claims in 2021, as well as other high-profile data breaches in similar industries and large businesses, and a wealth of relevant guidance and news reports at Defendant's disposal, Defendant knew or should have known that cybercriminals would target its electronic records and customers' PII.

45. These data breaches have been a consistent problem for the past several years, providing Defendant sufficient time and notice to improve the security of its systems and engage in stronger, more comprehensive cybersecurity practices.

46. PII is a valuable property right.[20] The value of PII as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory

---

[19] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Jan. 16, 2024).

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[21] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

frameworks."[22] American companies are estimated to have spent over $19 billion acquiring consumers' personal data in 2018.[23] In fact, it is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

47. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, and other PII directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

48. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[24]

49. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[22] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[23] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[24] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

50. Therefore, Defendant clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the PII stored in its unprotected files and the massive amount of PII it maintains.

Theft of PII has Grave and Lasting Consequences for Victims.

51. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of their financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[25]

52. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[26] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[27]

53. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact on their credit.

---

[25] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

[26] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[27] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Jan. 16, 2024).

54. Indeed, Plaintiff has already begun the long and arduous process of preventing further harm and injury resulting from the Data Breach. Mr. Abdellatif has spent time and money enrolling in identity theft protection services, which informed him that his Social Security information was on the "dark web." Plaintiff has suffered emotionally over the stress resulting from the Data Breach.

55. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[28] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim's credit rating.

56. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[29]

57. There may be a time lag between when PII is stolen and when it is used.[30] According to the GAO Report:

---

[28] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[29] *Id.* at 2, 9.

[30] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

58. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, Social Security Numbers, and other PII directly on various Internet websites, making the information publicly available.

59. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who companies employ to find flaws in their computer systems, stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[32]

60. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[33]

61. Plaintiff and Class members must vigilantly monitor their financial accounts and their family members' accounts for many years to come.

---

[31] U.S. GOV'T ACCOUNTABILITY OFF., *supra* n.28 at 29 (emphasis added).

[32] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[33] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited Jan. 16, 2024).

62. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

63. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (v) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

64. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

65. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All persons whose PII was accessed in the Data Breach by unauthorized persons.

66. Plaintiff reserves the right to amend the above definition or to propose other or additional classes in subsequent pleadings and/or motions for class certification.

67. Plaintiff is a member of the Class.

68. Excluded from the Class are AT&T, Inc., its affiliates, parents, subsidiaries, officers, agents, directors, the judge(s) presiding over this matter, and the clerks of said judge(s).

69. This action seeks both injunctive relief and damages.

70. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

71. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of Class members is unknown at this time, Class members are readily identifiable in Defendant's records, which will be a subject of discovery. Upon information and belief, there are millions of Class members in the Class.

72. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;
b. Whether Defendant's data security systems prior to the Data Breach met industry standards;
c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;
d. Whether Defendant breached its duty to Plaintiff and Class members to safeguard their PII;
e. Whether Defendant failed to provide timely and adequate notice of the Data Breach to Plaintiff and Class members;
f. Whether Plaintiff's and Class members' PII was compromised in the Data Breach;
g. Whether Plaintiff and Class members are entitled to injunctive relief; and
h. Whether Plaintiff and Class members are entitled to damages as a result of Defendant's conduct.

73. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and violations of law. Plaintiff and Class members all had their PII stolen in the Data Breach.

Plaintiff's grievances, like the proposed Class members' grievances, all arise out of the same business practices and course of conduct by AT&T.

74. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. His interests do not conflict with the interests of the Class.

75. Plaintiff and his chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG" or "Plaintiff's Counsel") -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint. In particular, FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. Plaintiff's Counsel are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class members. Finally, Plaintiff's Counsel possess the financial resources necessary to ensure that a lack of financial capacity will not hamper the litigation and is willing to absorb the costs of the litigation.

76. **Predominance.** The common issues identified above arising from Defendant's conduct predominate over any issues affecting only individual Class members. The common issues hinge on Defendant's common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

77. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large number of injured persons, to keep the courts from

becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class members can obtain the most compensation possible.

78. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which, in any event, might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class members, in terms of monetary damages due and terms of equitable relief, can be determined in this single proceeding rather than in multiple individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only customers of Defendant, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class members can be identified from Defendant's records, such that direct notice to the Class members would be appropriate.

79. **Injunctive relief.** Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

80. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

81. As a condition of receiving Defendant's products and/or services, Plaintiff and Class members were required to and did provide Defendant with their PII.[34]

82. By collecting and storing their PII and using it for commercial gain, at all times relevant, Defendant owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

83. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with statutory and industry standards and to ensure that its systems and networks and the personnel responsible for them adequately protected the PII.

84. Defendant knew the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted companies that store PII in recent years.

85. Given the nature of Defendant's businesses, the sensitivity and value of the PII it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

86. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them -- including Plaintiff's and Class members' PII.

---

[34] *See AT&T Privacy Notice*, *supra* n.14.

87. Plaintiff and Class members are a well-defined, foreseeable, and probable group of customers that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

88. Plaintiff and Class members have no ability to protect their PII that was or remains in Defendant's possession.

89. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

90. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

91. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to failing to adequately protect Plaintiff's and Class members' PII and failing to provide them with timely notice that their PII had been compromised.

92. Neither Plaintiff nor Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

93. By failing to provide timely and complete notification of the Data Breach to Plaintiff and Class members, Defendant prevented them from proactively taking steps to secure their PII and mitigate the associated threats.

94. As a result of Defendant's above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class

members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

95. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

96. Defendant had duties by statute to ensure that all information it collected and stored was secure and that it maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and Class members' PII.

97. Defendant's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

98. The FTC has published numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the personal customer

information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[35]

99. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses such as Defendant must take to meet their data security obligations and effectively put Defendant on notice of these standards.

100. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all Class members' PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores and the foreseeable consequences of a data breach involving PII, including, specifically, the substantial damages that would result to Plaintiff and other Class members.

101. Defendant's violation of the FTCA constitutes negligence per se.

102. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

103. The harm occurring as a result of the Data Breach is the type of harm against which Section 5 of the FTCA was intended to guard.

104. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt,

---

[35] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

105. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violation of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

106. Defendant's violation of the FTCA constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

107. Defendant owed a duty of care to Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

108. It was foreseeable that Defendant's failure to use reasonable measures to protect PII and provide timely notice of the Data Breach would result in injury to Plaintiff and other Class

members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

109. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF FIDUCIARY DUTY

110. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

111. Plaintiff and Class members gave Defendant their PII in confidence, believing that Defendant would protect that information. Plaintiff and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Defendant and Plaintiff and Class members.

112. In light of this relationship, Defendant has a fiduciary duty to act primarily for the benefit of Plaintiff and Class members upon matters within the scope of their relationship, which includes safeguarding and protecting Plaintiff's and Class members' PII.

113. Defendant breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII and otherwise failing to safeguard Plaintiff's and Class members' PII that it collected.

114. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (v) the continued risk to their PII which remains in Defendant's possession; and (vi) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

115. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

116. In connection with receiving products and/or services, Plaintiff and all other Class members entered into implied contracts with Defendant.

117. When Plaintiff and Class members paid money and provided their PII to Defendant, either directly or indirectly, as a pre-condition and in exchange for goods or services, they entered into implied contracts with Defendant.

118. Pursuant to these implied contracts, in exchange for the consideration and PII provided by Plaintiff and Class members, Defendant agreed to, among other things, and Plaintiff

understood that Defendant would: (1) provide products and/or services to Plaintiff and Class members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

119. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendant, on the other. Indeed, as set forth supra, Defendant recognized its duty to provide adequate data security and ensure the privacy of its consumers' PII by providing a privacy policy on its website.

120. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendant with their PII and paid for the services from Defendant.

121. Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of such an implied contract.

122. Had Plaintiff and Class members known that Defendant would not adequately protect its customers' and former customers' PII, they would not have received services from Defendant.

123. Defendant breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

124. Defendant's breach of its obligations under its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered.

125. Defendant's breach of implied contracts injured Plaintiff and all other Class members because (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

126. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

127. This claim is pleaded in the alternative to the breach of implied contract claim.

128. Plaintiff and Class members conferred a monetary benefit upon Defendant in the forms of (1) monies paid for services and (2) the provision of their valuable PII. Indeed, upon acquiring the PII, Defendant was then able to charge money for its services and utilize the PII for several purposes, including but not limited to advertising and marketing, providing its products and services, conducting consumer research, billing, and contacting customers.[36] The PII was thus used to facilitate payment and generate additional revenue for Defendant.

[36] *AT&T Privacy Notice*, *supra* n.14.

129. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Defendant profited from these transactions and used the PII of Plaintiff and Class members for business purposes.

130. Upon information and belief, Defendant, like most other corporate entities, funds its data security measures entirely from its general revenue, which includes money paid by Plaintiff and Class members.

131. As such, a portion of the payments made by or on behalf of Plaintiff and Class members is or should have been used to provide a reasonable level of data security.

132. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure its customers' PII.

133. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant avoided its data security obligations at the expense of Plaintiff and Class members by utilizing less expensive and less effective security measures.

134. As a direct and proximate result of Defendant's failure to provide the requisite security, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

135. Defendant should not be permitted to retain the money belonging to Plaintiff and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

136. Defendant should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of its conduct and the resulting Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in his favor and against Defendant as follows:

A. Certifying that Class as requested herein, appointing the named Plaintiff as Class representatives and the undersigned counsel as Class Counsel;

B. Requiring that Defendant pays for notifying the members of the Class of the pendency of this suit;

C. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

D. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiff and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiff and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: April 10, 2024

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214/744-3000 / 214/744-3015 (fax)
jkendall@kendalllawgroup.com

Todd S. Garber (*pro hac vice forthcoming)*
Andrew C. White (*pro hac vice forthcoming)*
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Attorneys for Plaintiff and the Proposed Class